REMARKS

Applicants acknowledge that the Office Action dated January 30, 2006, has been made Final. Nevertheless, the changes made by the foregoing amendment are formal in nature, and are intended to increase the readability of claim 1, without altering its substantive content. Therefore, the amendments thus made do not require further search or consideration by the Examiner. Accordingly, entry of the foregoing amendment is respectfully requested pursuant to Rule 116. More particularly, if the Examiner maintains the final rejection of claims 1-12, entry of the foregoing amendment is requested in order to place this application in better form for appeal.

Claims 1 and 3-12 have been rejected under 35 USC §102(b) as anticipated by Gabber et al. (U.S. Patent No. 5,961,593). In addition, claim 2 has been rejected under 35 USC §103(a) as unpatentable over Gabber et al. in view of Binding et al. (U.S. Patent No. 6,694,431). However, for the reasons set forth hereinafter, applicants respectfully submit that all of claims 1-12, which are currently being examined in this application, distinguish over the cited references, whether considered separately or in combination.

The present invention is directed to a method for enhancing the privacy and security of an individual who uses a web browser to download and display information from the internet. In particular, the invention relates to the use of a terminal which, for whatever reason, may be subsequently accessed by a

different person, who can obtain information stored by the web browser software on the hard disk of that terminal during its use by the previous user.

As is known to those skilled in the art, a browser software program routinely stores on the hard drive of the terminal in which it is located, information relating to web pages that a user has visited, as well as other information, such as passwords, user names, cached web pages and the like. As noted at page 2 of the specification, although the storage of such information facilitates internet browsing, there are circumstances in which the stored information may be accessible to unauthorized persons, thus presenting a security and privacy risk. In particular, where a PC may change ownership, or be used by multiple users, such as in public internet facilities, it is possible that a subsequent user of the PC may, by examining the contents of the hard drive, obtain information which is stored by the browser/software for a former user during a web browsing session. A scenario in which such unauthorized access might occur is described in the specification at page 7, line 2, through page 8, line 23.

The present invention addresses and resolves this problem by providing a system in which a user may use a browser running in an "untrusted" environment (such as a PC in a public or multi-user facility) to visit a remote trusted website, and download from the website a further browser (referred to in the claims as a "communications application"), which the user knows to have been configured to browse the internet without caching or otherwise storing data

on the hard disk of the PC. Having thus downloaded the trusted browser, the user may use it to browse the internet, secure in the knowledge that no residue of information will be left on the hard drive of the public terminal, which might be improperly accessed by a subsequent user. (See, for example, page 10, lines 8-17.)

Both the present invention and Gabber et al. are directed to methods for increasing the anonymity and privacy of users of the internet. However, while the present invention enhances privacy and security in one way (by eliminating the possibility that a subsequent user of a multi-user PC might improperly access information stored thereby a web browser during a previous web browsing session), Gabber et al. avoids sending data which could be used to identify or track a user to network locations, by providing network browsing through a proxy server or the like, which masks identifying data before transmitting it to the visited sites. Thus, the present invention is not concerned with the issue of transmitting identifying or sensitive information to remote network sites, and Gabber et al. is not concerned with traces of browsing activity left behind on a user terminal. Accordingly, the present invention and Gabber et al. provide very different solutions to very different problems.

The Office Action states that Gabber et al. discloses a step of "receiving the communications application at the terminal" (emphasis added), referring to the receipt of "substitute identifiers," as discussed at column 6, lines 17-51. Such substitute identifiers are simply alternative identifiers which are generated by a

central proxy system from data specific to users, and are transmitted to a remote site in place of the actual identifiers which could be traced to the user whose anonymity is to be preserved. Thus, the Office Action equates the "communications application" recited in claim 1 of the present application with the "substitute identifiers" in Gabber et al.

Applicants respectfully submit, however, that the latter two are quite different from each other. That is, as can be determined from a review of the specification of the present application, the term "communications application" refers to web browsing software. (See, for example, page 10, lines 8-14, which refers to a user's visiting a remote trusted website and downloading "a further browser" which is known to the user to have been configured to browse the internet without caching or otherwise storing data on the hard disk of the PC.) It is apparent, however, that the "substitute identifiers," such as user names and passwords, as discussed at column 2, lines 13-19, of Gabber et al., are merely labels which are generated by the server, and are not downloaded to the user terminal at all. In fact, quite the reverse is true. They are generated by the server and transmitted to a viewed site. They will not be seen by the user terminal, and they are not equivalent to communications software.

In view of the above, applicants respectfully submit that Gabber et al. does not teach or suggest the following features of the invention as included in claim 1 of the present application:

1. Transmitting to a remote server a request for a communications application.

Feature 110a in Figure 2 represents a central proxy site (column 5, lines 25-26) which provides substitute identifiers (data) to a remote site 110g (column 5, lines 58-63). No communications application software is requested by the user terminal (105a).

2. A communications application stored on the server to be downloaded to a terminal connected to the network.

Figure 2 does not illustrate any downloading to the user terminal 5. Rather, it illustrates user terminal 105a connected to remote site 110g through a proxy site 110a which generates substitute identifiers that prevent remote site 110g from identifying the user at user terminal 105a. The abstract discusses browsing of remote network sites 110g by a user 105a through a proxy 110a which communicates with remote network site 110g using substitute identifiers. It does not describe a request for a communications application to be downloaded to the user terminal 105a. The passage at column 5, line 47 to column 6 , line 17, discusses the provision of substitute identifiers by proxy system 110a to remote site 110g, and the removal of identifying portions of browsing commands transmitted by the user 105a before sending them to remote site 110g. It does not describe downloading anything, much less a communications software application, to the user terminal 105a.

3. Receiving the communications application at the terminal.

The cited passage at column 6, lines 17-51, discloses that parts of the substitute generation task may be performed at the user site 105a. There is no disclosure of downloading the required software from a server, but in any case, software required to perform the described first and second routines does not constitute a "communications application." At most, the first and second routines within the user site may operate to generate data (substitute identifiers) to be used by a communications application such as a network browser.

4. User input data, which is input to the communications application by a user of the terminal, is transmitted into the network without storing a record of the data at the terminal.

User input data is only transmitted into the network of Gabber et al. in embodiments where the first and second routines are performed at a remote network server as shown at 110a in Fig. 2. The user input data, input to the communications application by a user of the terminal is only transmitted as far as the proxy site 110a. Gabber provides no discussion of whether or not a record of the transmitted data is stored at the user terminal. The "anonymous" browsing provided by Gabber means simply that a browsed network site will not be able to identify the user. The present invention is not concerned with personal information transmitted into the network; rather, it is concerned with

personal information left stored on the user terminal after the user has finished browsing.

Regarding claim 3, the generated substitute identifiers are used by a conventional communications application to communicate with remote sites.

Regarding claim 4, the inlaid interface described at column 8, liens 17-21, operates within a conventional communications application, not one which is downloaded by the method of Gabber et al. The inlaid interface prompts for the input of data to the substitute identifier generating routines, and forwards input data to the substitute identifier generating routines by conventional operation of the conventional communications application. The cited passages (column 7, liens 19-61 and column 8, liens 3-63) do not describe one communications application running within another.

Regarding claim 7, the cited passages discuss a user browsing a remote site through a proxy system which generates substitute identifiers, but do not describe browsing via a web browser running on the proxy system.

Regarding claim 8, the cited passages discuss a user browsing a remote site through a proxy system which generates substitute identifiers, but do not describe browsing via a web browser running on the proxy system. There is no discussion of web pages being presented in non-graphical format from a web browser application.

Regarding claims 9-10, Gabber et al. makes no mention of avoiding the storage of data transmitted to the network on the user terminal. The passages

cited refer to the reception of user data from a user terminal and the resulting generation of substitute identifiers for transmission across the network.

Accordingly, for the reasons set forth hereinabove, applicants respectfully submit the invention as defined in claims 1-12 distinguish over the cited references.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 038819.53225US).

Respectfully submitted,

May 1, 2006

Gary R. Edwards
Registration No. 31,824

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:aw

2761271